Lawrence Somer and Michal Křížek

Identically Distributed Second-Order Linear Recurrences Modulo p, II, Fibonacci Quart. 54 (2016), no. 3, 217–234.

Abstract

Let p be an odd prime and let u(a, 1) and u(a', 1) be two Lucas sequences whose discriminants have the same nonzero quadratic character modulo p and whose periods modulo p are equal. We prove that there is then an integer c such that for all $d \in \mathbb{Z}_p$, the frequency with which d appears in a full period of $u(a, 1) \pmod{p}$ is the same frequency as cd appears in $u(a', 1) \pmod{p}$. Here u(a, 1) satisfies the recursion relation $u_{n+2} = au_{n+1} + u_n$ with initial terms $u_0 = 0$ and $u_1 = 1$. Similar results are obtained for the companion Lucas sequences v(a, 1) and v(a', 1). We also explicitly determine the exact distribution of residues of $u(a, 1) \pmod{p}$ when u(a, 1) has a maximal period modulo p.